LéLaw Thought Leadership Insights

April 2021

Examinations:

Data Subjects' Rights Under The Nigerian Data Protection Regulation 2019

Thought Leadership by:

Sam Ngwu[1]

s.ngwu@lelawlegal.com

Humans were created naturally to dominate their environment, and part of their evolutionary quest in this regard has been the creation of the computer, internet and later day artificial intelligence (AI), internet of things (IoT) and Blockchain (BC). We live in a digitised world. Businesses and organisations deploy data analytics to derive insights with which they make decisions about their consumers and enterprises. As beautiful as this may sound, the world is becoming unsafe for data subjects[2] (DS) because the more our world is digitised, the more users' data is processed and our privacy endangered.

The extensive processing of data[3] could jeopardise DS data and infringe on their rights if specific laws and safeguards are not implemented. The use of artificial intelligence (AI) such as facial recognition could create racial discrimination, while deepfakes lead to misrepresentation and harassment of people.[4] The use of social media exposes us to many online threats- cyberbullying, extracting consents, overexposure and faithless friend.[5] The IoT creates vulnerability to online attack and hackings.

WhatsApp introduced a new privacy policy to share more commercial user data with its parent, *Facebook*.[6] Many people saw this as a further impingement on the privacy of the users/subscribers. To ensure that data is lawfully collected and adequate measures established to protect users, the European Union passed ***General***

1 The author is grateful for the respective helpful comments of Messrs Ridwan Oloyede and Chuks Okoriekwe to a prior draft of this article. However, the author is fully responsible for all the views expressed herein, including all and any errors.

2 ***Article 1.3(xiv) NDPR*** defined "*Data Subject*" "*as any person, who can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*".

3 By ***Article 1.3(iv),*** "*Data*" "*means characters, symbols and binary on which operations are performed by a computer, which may be stored or transmitted in the form of electronic signals, stored in any format or any device.*"

4 Prof. Woodrom Hartzog, ***'Fundamentals of Privacy Law',*** *Coursera:* https://www.coursera.org/learn/ northeastern-data-privacy/lecture/PBTt9/lesson-4-artificial-intelligence (last accessed 14.01.2021).

5 Prof. Woodrow Hartzog, ***(supra).***

6 The new privacy policy generated much muse from the public domain prompting very many people to migrate to an alternative social media. The massive outcry made WhatsApp (on Tuesday, 12.01.2021) to clarify that they do not share personal chat messages with parent company Facebook; "*instead the update includes changes related to messaging a business on WhatsApp, which is optional ,and provides further transparency about how we collect and use data.*" See ETtech, ***'After Backlash, WhatsApp Clarifies Its New Privacy Policy',*** *The Economic Times/Tech, 14.01.2021:* https://economictimes.indiatimes.com/tech/technology/after-facing-backlash-whatsapp-clarifies-its-new-privacy-policy/articleshow/80226028.cms (last accessed 14.01.2021).

Data Protection Regulation 2018 (GDPR).[7] Sequel to this, Nigeria followed suit by releasing the ***NDPR*** in 2019 to protect the rights of (DS). In the light of the above, this article seeks to examine the rights of DS under the ***NDPR*** to explore the extent of protection accorded users and enforcement mechanism in cases of breach whilst highlighting compliance obligations on DC and PD.

UNDERSTANDING THE RIGHTS OF DATA SUBJECTS

In many developed countries, the right to data protection (DP) is a fundamental human right (FHR).[8] In Nigeria, the position seems unsettled, with two emerging schools of thought. The first believes that DP is an extension of the right to privacy as provided in the ***1999 Constitution***[9] and an FHR. The second school of thought argues strongly that DP is not privacy and cannot amount to FHR under section 37 of the constitution.[10]

Whatever the case, DS is entitled to some rights against misuse, abuse, and unlawful processing of their data. These rights apply to only human persons and not to artificial legal persons.[11] Therefore, data belonging to corporations are not protected under the ***NDPR.*** However, the PD of the company's alter ego is protected. These rights are identified as follows:

1. Right to be informed of the processing

Any data controller (DC) wanting to collect, use, consult or process personal data[12] (PD) of DS must inform such DS about the processing and its extent.[13] This means that companies, institutions or individuals must tell DS what data they are processing and the purpose for such processing in *a clear, plain, concise, transparent and intelligible manner*. It is a key manifestation of the transparency principle that suggests that DC must be open and provide clear and concise information about what is done with their data.

The information shall be in writing, or other means, including, where appropriate, by electronic means.[14] When requested by the DS, the information may be provided orally, provided that the identity of the DS is proven by other means. The information to be provided by the Controller includes the identity of DC, contact of Data Protection Officer (DPO), the purpose of processing, the legitimate interest pursued by the DC or the third party; period of storage, recipients or categories of recipients and the existence of other rights.[15] *"The risk inherent with processing data of data subjects without their knowledge is the tendency to subject them to discrimination or disadvantages and prevent them from exercising their rights"*.[16] Complying with the right is essential to foster trust in public institutions and give private organisations an edge over competitors.[17]

7 The ***GDPR*** replaced the ***Data Protection Directive*** established in 1995 to cater for transformation that has taken place, ensure uniform regulation within the European Union and extraterritorial applicability.

8 ***Article 1(2) GDPR 2018.***

9 ***Section 37 1999 Constitution of the Federal Republic of Nigeria as amended (1999 Constitution).***

10 Olumide Babalola, ***'Privacy Versus Data Protection Debate in Nigeria: The Two Schools of Thoughts'***, *Thenigerialawyer.com,31.01.2021*:https://thenigerialawyer.com/privacy-versus-data-protection-debate-in-nigeria-the-two-schools-of-thought/ (last accessed 10.02.2021).

11 ***Article 1.1(a) and 1.2(b).***

12 ***Article 1.3(xix).*** *" 'Personal Data' means any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifier such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM, Personal Identifiable Information (PII) and others."*

13 ***Article 3.1(1) NDPR 2019.***

14 Such as using a layered approach, dashboard, pop ups, voice alert, icon etc.

15 ***Article 3.1(7)(a)-(e) NDPR 2019.***

16 European Union Information Commissioner's Office (ICO), ***'Guide to the General Data Protection Regulation (GDPR)'***:https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-dataprotection-regulation-gdpr/the-right-to-be-informed/what-is-the-right-to-be-informed-and-why-is-itimportant/#what1 (last accessed 23.02.2021).

17 ICO, ***(supra)***.

2. Right of access

A DS has a right to access their data and obtain a copy of their PD, and other supplementary information from an organisation processing PD, which may or may not include payment of a fee depending on the circumstances of the case;[18] provided such access will not infringe on the right of others. The right is exercised through Data Subject Access Request (DSAR), and the essence is to bring to fore why and how data belonging to the DS are used and to check if the processing is lawful.[19] Thus, ***Paragraph 3.2(xi) of NDPR Implementation Framework 2020*** enjoins DC to design their systems and processes to make data requests and access seamless for DS.

For instance, students (DS) based on this right can request their school or other institution that has their information to provide such information to them at no cost. According to a writer: *"An individual is* ***only entitled to access the personal data about them****, and not the information relating to other people (unless he/she is acting on behalf of someone). Therefore, it is crucial to establish whether the information requested falls within the definition of personal data".*[20]

The right as postulated gives life to other rights such as rectification, erasure or objection to further processing.[21] This is because DS first need to gain access before they can erase, rectify or object as the circumstances may require. ***NDPR*** did not provide the form the request can be made. Consequently, it can be in writing or oral, including social media, provided it presents a clear intention of the DS to ask for their PD. ***NDPR*** did not provide that a third party relative, friend or solicitor can request DS and what happens when the request affects the third party.

However, according to ***Information Commission Office(ICO) Guide to GDPR,*** a third party-relative, friend or solicitor can be instructed by the DS to make a request on their behalf[22] and where the information requested affects a third party and the possibility of disclosing such information without necessarily revealing that other third party's information is not forseeable, request may not be complied with except consent is obtained from the third party.[23] The time limit for a response was not factored in the ***NDPR***. Still, DC is expected to inform DS within one Month, reason for not taking action and on the possibility of lodging complaints with a supervisory authority.[24] The information requested should be provided in an accessible, concise and intelligible format.

Reasonable effort should be exerted towards finding and retrieving the requested information provided searches would not be unreasonable or disproportionate to the importance of providing access to the information. Aside this, access can also be refused if it is manifestly unfounded or excessive. DS should be informed the reason for the refusal and their right to seek enforcement in court or from the Supervisory Authority.

3. Right to Request Deletion

The ***NDPR***'s ***Articles 3.1(9)*** and ***(7)(h)*** empowers DS to request that

18 ***Article 3.1(7)(h) NDPR 2019.*** Further, ***Article 1.3(xv)*** provides " *'Data Subject Access Request' means the mechanism for an individual to request a copy of their data under a formal process which may include payment of a fee'. The circumstances where fee may be charged include where the request is manifestly unfounded or excessive, or if an individual requests further copies of their data.*``

19 Professor Lydia F de la Torre, **'Right of Access and SARS Under the EU Data Protection Law'**, *Golden Data, 21.02.2019:* https://medium.com/golden-data/what-is-the-right-to-access-under-eu-data-protection-law-a917260552d6 (last accessed 12.02.2021).

20 *Ibid.*

21 ***Ibid***

22 ICO, ***(supra).***

23 ICO, ***(supra),*** *p. 103.*

24 ***Article 3.1(2) NDPR.***

their PD be deleted or erased. This is also known as right to be forgotten or de-referencing. This right creates an opportunity for DS to make mistakes without fear of old mistakes or failures coming back to haunt them. For instance a person who no longer wants to operate a particular social media account can request the host to delete the account.

This right is not absolute and only applies in certain unique circumstances such as, where: (a) the PD are no longer necessary in relation to the purposes for which they were collected or processed; (b) the DS withdraws consent on which the processing is based; (c) the DS objects to the processing and there are no overriding legitimate grounds for the processing; (d) the PD have been unlawfully processed; and (e) the PD must be erased for compliance with a legal obligation in Nigeria.

Where PD was divulged to others, steps must be taken to contact the controllers and inform them about the request to delete.[25] If the request to delete is received without any exemption, both the live and backup systems must be deleted and the implication clearly communicated to the DS.[26] If an exemption is made for data in the backup system, it must not be used for any other purpose until it is overwritten.

Whilst the ***GDPR's Article 17(3)*** provides several exceptions[27] to this right, ***NDPR's Article 3.1(7)(h)*** has no exception. Nonetheless, we can rightly assume that outside the circumstances listed in (a-e) above, the right to delete can be refused. ***NDPR*** did not specify the form the request should take, therefore, it can be made orally or in written form to any part of the organisation.[28] An employee of an organisation can receive the request on behalf of the organisation. However, It is advised that the information be given to the management of the institution.

In ***Google Spain, Google Inc. v. Agencia Espanola de Proteccion de Datos (AEPD) & Mario Costeja***,[29] the CJEU held that data subjects have a right to erasure or, more specifically, to remove any links shown by the search engine to their names. The Court acknowledged the fact that the processing of personal data, such as those of Mr. Costeja, is liable to significantly affect the fundamental rights to privacy and data protection when it is possible to search for an individual using his or her name. However, where this right will infringe on freedom of expression or there is a general public interest to have access to this information such as when DS are prominent figures in the public life and information about them must be known to those who are interested in it. [30]

4. Right to restrict processing

DS has the right to restrict the processing of PD in stated circumstances.[31] These are, where the: (a) accuracy of the PD is contested by the DS for a period enabling the Controller to verify the accuracy of the PD (b) processing is unlawful, and the DS opposes the erasure of the PD and requests the restriction of their use instead; (c) controller no longer needs the PD for the purposes of the processing, but they are required by the DS for the establishment, exercise or defence of legal claims; and (d) DS has objected to processing, pending the verification whether the legitimate grounds of the Controller override those of the DS.

For instance, a school website may mistakenly list a DS as a second class honours student, instead of first class that such DS actually had. The DS has the right to request restriction of further processing of personal information pending the verification of the accuracy of the information by the school. This

25 ***Article 3.1(10) NDPR.***
26 ICO, ***(supra)***, *p.114.*
27 The exceptions include where processing is necessary to exercise the right of freedom of expression and information; to comply with legal obligation; for performance of a task carried out in the public interest or in the exercise of official authority; for archiving purposes in the public interest, scientific research, historical research or statistical purposes where the deletion is likely to render impossible or seriously impair the achievement of that processing; or for the establishment, exercise or defence of legal claims.
28 **ICO, *(supra), p.117.***
29 ***ECLI: EU: C: 2014:317***: https://eur-lex.europa.eu/legal-content /EN/TXT/?uri=CELEX%3A62012CJ0131 (last accessed 22.02.2021).
30 University of Groningen ***'Understanding The GDPR',*** *Future Learn,* https://www.futurelearn.com/ courses/general-data-protection-regulation (last accessed 5.2.2021).
31 ***Article 3.1(11) and 3.1(7)(h) NDPR.***

right may serve as an alternative option to the right for erasure and closely linked to the right for rectification and objection. A DS who challenges accuracy and seeks rectification of PD can, at the same time, request restriction of the processing pending such rectification or objection.

Where processing is restricted, it cannot be reopened without the consent of the DS except in the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest in Nigeria.[32]

In circumstances, that the data are disclosed to others, effort must be made to inform them about the restriction placed on processing of PD. As earlier discussed, ***NDPR*** did not provide the format request for restriction should be. This leaves it open to any permissible format whether to be in writing or oral form including social media depending on the circumstances of the case.

5. Right to portability

Data Portability simply means the ability to transfer data from one IT system or computer to another through a safe and secured means in a standard format.[33] DS have the right to receive from controllers PD concerning them in a structured, commonly used and machine-readable format and to transmit these data to other controllers without hindrance provided: firstly, the processing is based on consent, or secondly, on a contract, and thirdly, the processing is carried out by automated means (excluding manual files).[34]

If it is technically possible, PD can be directly transmitted from one Controller to another provided that this right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller.[35] In essence, this gives the DS free will to manage and reuse their PD. Thus, a DS can copy his data in *Facebook* to *twitter* or other IT platforms and *vice versa*, seamlessly.

6. Right to object to processing

Every user has the right to object to processing of PD at any material time.[36] The objection may be with respect to particular PD or to all of the PD or to a particular purpose data is being processed. An individual can object to the processing of their PD for direct marketing at any time including profiling. The Controller must ensure a mechanism for objection free of payment. This right prevails on the Controller to stop from further processing of PD. A DS who does not want to be receiving direct marketing mail can object to it without necessarily being deprived of the right to access the website. A face-it or leave it option will amount to data breach.[37]

Right to object to processing can be expressed in any form, oral or in writing including social media and conveyed to any part of the organisation. The execution of the objection must be done within one month, all things being equal.[38]

7. Right to rectification

By ***Article 3.1(7) (h), (8)*** and ***(13) NDPR*** DS are entrusted with the right to correct inaccurate PD without undue delay and have incomplete PD completed subject to the purposes for the processing. This may include making available the supplementary statement to the incomplete data. Irrespective of the steps taken *ab initio* to ensure accuracy of data by Controller, once a request for rectification is made, an obligation is imposed on

32 ***Article 3.1(12) NDPR.***
33 ***Article 1.3(xii) NDPR.***
34 ***Articles 3.1(14)*** and ***(7) (h) NDPR.***
35 ***Article 3.1(15) NDPR.***
36 ***Articles 2.8 and 3.1(7)(h) NDPR 2019.***
37 Prof. de La Torre, ***(supra).***
38 ***Article 3.1(2) NDPR.***

the Controller to timely reconsider the accuracy of the data.

The ***NDPR*** does not define "*inaccuracy*". However, under the ***UK Data Protection Act 2018***, PD is inaccurate if it is incorrect or misleading as to any matter of fact. The issue of determining inaccurate data is a very complex one. For instance where a data refers to a mistake that has subsequently been resolved, it may be possible to argue that the record of the mistake is in itself accurate and should be kept. [39]

However, the fact that a mistake was made and the correct information has been included in the individual's data should be expressed. Once a request for rectification is made, the DC is expected to restrict processing pending verification of the accuracy of the data whether or not DS exercises right to restriction. DC can refuse rectification if satisfied that the PD is accurate, but must inform DS the reason behind the decision and their right to make a complaint to court or Supervisory Authority.

The ***NDPR*** did not specify the form (whether in writing or verbally) the request for rectification can be made in any form and to any part of the organisation including the employee. It needs not possess the phrase "*request for rectification*" or the relevant articles of the regulation to be a valid request. It will suffice once the content challenges the accuracy of the PD in issue. Where data was disclosed to a third party, steps must be taken to inform them about the rectification provided such steps will not amount to disproportionate effort.

8. Right to withdraw consent

The condition of a freely given consent attracts to itself right to withdraw such consent. DS have a right flowing from the right to consent to withdraw whatever consent they have given provided such withdrawal does not affect lawful processing which took place prior.[40] The DS shall be informed prior to giving consent that they possess similar right to withdraw consent and that it shall be easy to withdraw such consent. "*In principle, consent can be considered to be deficient if no effective withdrawal is permitted*".[41] The basis of consent to PD processing is to grant individuals with autonomy to freely elect how others can use their personal information.[42]

Even though ***NDPR*** did not provide means of withdrawing consent, it has been contended that consent can be withdrawn through any of these means: a termination of a user account, uninstallation of a game or other way of ending the usage of a service.[43]

9. Right in relation to automated decision making and profiling.

Automated individual decision making is a decision made by automated means without any human intervention such as an online decision to award a loan or a recruitment aptitude test which uses pre-programmed algorithms and criteria.[44] While automated individual decision-making often involves profiling, it does not have to always be. ***NDPR*** requires the Controller to inform the DS prior to processing of PD, the existence of automated decision-making, including profiling and at least, in those cases, meaningful information about the logic involved as well as the significance and the envisaged consequences of such processing for the DS.[45]

NDPR did not define the meaning of profiling. However, under the ***GDPR***[46] it is defined as "*any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects*

39 ICO, ***'Guide to the General Data Protection Regulation (GDPR)', ICO***: https://ico.org.uk/fororganisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to rectification/(last accessed 23.02.2021). As rightly provided under the ***Guideline*** as an example (at *p. 108*): "*If a patient is diagnosed by a GP as suffering from a particular illness or condition, but it is later proved that this is not the case, it is likely that their medical records should record both the initial diagnosis (even though it was later proved to be incorrect) and the final findings. Whilst the medical record shows a misdiagnosis, it is an accurate record of the patient's medical treatment. As long as the medical record contains the up-to-date findings, and this is made clear in the record, it would be difficult to argue that the record is inaccurate and should be rectified.*"

40 ***Articles 2.3(2)(c) and 3.1(7)(i) NDPR 2019.***

41 Wp29, ***'Opinion No. 15/2011 on the Definition of Consent', 01197/11/EN and WP187***, *13.07. 2011, p. 13,* cited in J.Misek, ***'Consent to Personal Data Processing-The Panacea or The Dead End?',*** *Masaryk Univ. Journal of Law and Tech (Vol.14, No.2, 2020), p.74:*https://journals.muni.cz/mujlt/index (last accessed 22.02.2021).

42 J.Misek, ***(supra)***, *p.74.*

43 *Ibid.*

44 ICO, ***(supra)***, *p.153.*

45 ***Article 3.1(7)(l) NDPR 2019.***

46 ***Article 4(4) GDPR 2018.***

concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements". In essence organisations collect personal information of DS from different sources and with the help of AI classify individuals into different groups or sectors. This analysis identifies links between different behaviours and characters to create profiles for individuals.[47]

Organisations use profiling to find something about individuals' preferences, predict their behaviours; and /or make decisions about them. Automated individual decision-making and profiling can lead to quicker and more consistent decisions. But if they are used irresponsibly it will amount to significant risks for individuals.[48] Therefore, controllers are restricted from conducting automated decisions including profiling that portends certain significant effects on individuals without their consent.

10. Right to lodge complaint with the regulator

Article 3.1(7) (j) NDPR empowers DS to lodge complaints to the National Information Technology Development Agency (NITDA) whenever breach of their data rights are occasioned. The Agency upon receipt of the complaint will constitute an Administrative Redress Panel (ARP) to conduct investigation and determine appropriate redress within 28 working days.[49] An administrative order may be issued to protect the subject-matter of the allegation pending the outcome of the investigation.[50] In furtherance, a 15 member Data Breach Investigative Team (DBIT) was inaugurated by the NITDA Director-General to carry out investigations on breach of ***NDPR***.[51] The Agency is only entitled to award penalty in terms of fine and may not grant remedy to DS as the regulation does not provide for remedies.[52] Nevertheless, this does not prejudice the right of DS to approach court for remedies.[53]

CONCLUSION

As the foregoing discussion shows, the rights offered to DS in Nigeria by the ***NDPR*** are not well knitted and encompassing. Unlike in the ***GDPR***, there are no clear cut exceptions to some of these rights, and the form that exercising them should take. Also, the ***NDPR*** did not provide remedy for DS where these rights are breached. It is hoped that the ***Nigerian Data Protection Bill 2020 (NDPB)*** will provide sufficient answers to many gaping questions on these issues. Notwithstanding, ***NDPR*** must be commended for providing these rights and opening up the space which will be consolidated upon by subsequent enactments.

47 *ICO, (supra), p.153.*
48 *ICO, (supra). p.153*
49 *Article 4.2 NDPR 2019.*
50 *Article 4.2(4) NDPR 2019.*
51 The investigative team is believed to have investigated an online betting company reported to have breached ***NDPR***.
52 ***Article (4.2)(6) NDPR 2019.*** The article provides that a breach of NDPR is a breach of ***NITDA Act 2007*** and by ***sections 17*** and 18, any breach of the ***NITDA Act*** will amount to a criminal offence.
53 ***Article (4.2)(1) NDPR 2019.***